

CLAIMS

What is claimed is:

1. A computerized method by which a ticket provider may deliver a digital ticket to a ticket consumer across a communications channel, which digital ticket is subject to subsequent redemption, the digital ticket computerized delivery and redemption method comprising:

first communicating, across a communications channel from a computer of a ticket provider to a computer of a prospective ticket consumer, first digital data D_1 in respect of an occurrence for which tickets may be delivered; and then, the prospective ticket consumer deciding to obtain a digital ticket for the occurrence and thus to become a ticket consumer,

second communicating, across the communications channel from the computer of the ticket consumer to the computer of the ticket provider, second digital data D_2 including indication that a ticket is desired for the occurrence; and then, the ticket request being capable of being fulfilled,

calculating in the computer of the ticket provider by use of a private key s a digital signature of third digital data D_3 , which third digital data D_3 is in respect of one or both of the first digital data D_1 and the second digital data D_2 , which digital signature of the digital data D_3 is, as well being a proof both (i) that a private signature key s was used by the computer of the ticket provider in generation of the digital signature and (ii) that one or both of the digital data D_1 , D_2 was used in respect of its generation, (iii) suitably stored in a transportable storage medium;

wherein the digital data D_1 , D_2 in respect of which the digital signature of digital data D_3 was generated becomes a memorialization of a particular provision by the ticket provider of the particular digital ticket for the particular occurrence to the

ticket consumer who is particularly identified at least as a party at the other end of the communicating transpiring across the communications channel;

third communicating, across the communications channel from the computer of the ticket provider to the computer of the ticket consumer, at least the signed digital data D_3 ;

first storing with the computer of the ticket consumer in the transportable storage medium at least the signed digital data D_3 , thus turning the transportable storage medium into a digital ticket;

physically transporting the digital ticket in the form of the transportable storage medium so containing at least the signed digital data D_3 to a specific time and place where the specific occurrence for which the digital ticket has been provided is to transpire;

tendering the digital ticket for redemption to a ticket taker at the specific occurrence;

reading into a computer of the ticket taker at least the signed digital data D_3 ;

recovering in the computer of the ticket taker, with a digital verification key ν corresponding to the signature key s of the ticket provider and from the signed digital data D_3 , the digital data D_3 ; and

determining in the computer of the ticket taker IF the digital data D_3 was recoverable by verification key ν AND, having been so recovered, the digital data D_3 correctly memorializes the particular provision by the ticket provider of the particular third digital data D_3 for the particular occurrence to the particular ticket consumer who at one time communicated across the communications channel THEN the digital ticket is valid, ELSE IF the digital data D_3 was recovered by use of the verification key ν BUT the digital data D_3 recovered incorrectly memorializes the particular provision by the ticket provider of the particular third

digital data D_3 for the particular occurrence to the particular ticket consumer who at one time communicated across the communications channel THEN the digital ticket is invalid.

2. The digital ticket computerized delivery and redemption method according to claim 1

wherein the second communicating is of second digital data D_2 including a one-way function **hash(R)** of a number **R** which number **R** is uniquely known to the computer of the ticket consumer and not to the computer of the ticket provider;

wherein the calculating in the computer of the ticket provider is of a digital signature in respect of the third digital data D_3 including the one way function of **hash(R)** plus information **I** concerning the event for which the ticket is had, **Sign(s, I || hash(R))**;

wherein the third communicating is of **Sign(s, I || hash(R))**;
wherein the first storing is of **R** appended to **Sign(s, I || hash(R))**, or **Sign(s, I || hash(R)) || R**, as the digital ticket;

wherein the reading into the computer of the ticket taker is of the **Sign(s, I || hash(R)) || R**;

wherein the recovering in the computer of the ticket taker of the **I || hash(R)** gives **hash(R)**; and, having both **R** and **hash(R)** to hand,

wherein the determining further proceeds by recalculating the **hash(R)** in respect of **R**, so that IF the recalculated **hash(R)** equals to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is valid ELSE IF the **hash(R)** does not equal to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is invalid.

3. The digital ticket computerized delivery and redemption method according to claim 2

wherein the determining still further proceeds so that IF the read digital ticket is the first uniquely presented THEN the digital ticket is valid ELSE IF the read digital ticket is not the first uniquely presented THEN the digital ticket is invalid.

5 4. The digital ticket computerized delivery and redemption method according to claim 2

wherein the second communicating is of a one-way hash function **hash(R)** of a number **R**;

10 wherein the calculating in the computer of the ticket provider is of a digital signature in respect of signature key **s** of both the **hash(R)** plus information **I** concerning the event for which the ticket is had, **Sign(s,I||hash(R))**;

wherein the third communicating is of **Sign(s,I||hash(R))**;

15 wherein the first storing is of **R** appended to **Sign(s,I||hash(R))**, or **Sign(s,I||hash(R))||R**, as the digital ticket;

wherein the reading into the computer of the ticket taker is of the **Sign(s,I||hash(R))||R**;

20 wherein the recovering in the computer of the ticket taker of the **I||hash(R)** gives **hash(R)**; and, having both **R** and **hash(R)** to hand,

25 wherein the determining further proceeds by recalculating the **hash(R)** in respect of **R**, so that IF the recalculated **hash(R)** equals to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is valid ELSE IF the **hash(R)** does not equal to the recovered **hash(R)** of the digital ticket as read THEN the digital ticket is invalid.

5. The digital ticket computerized delivery and redemption method according to claim 4

30 wherein the determining still further proceeds so that IF the read digital ticket is the first uniquely presented THEN the

digital ticket is valid ELSE IF the read digital ticket is not the first uniquely presented THEN the digital ticket is invalid.

6. The digital ticket computerized delivery and redemption method according to claim 1

5 wherein the calculating is of digital signature suitably displayed as a 2-D code; and

wherein the first storing with the computer of the ticket consumer is by printing of the 2 -D code upon a printable transportable storage medium.

10 7. The digital ticket computerized delivery and redemption method according to claim 6 wherein the reading into a computer of the ticket taker of the digital signature transpires by use of an optical reader.

15 8. A computerized method by which a ticket provider may deliver a ticket to a ticket consumer across a communications channel comprising:

first transmitting, across a communications channel from a computer of a ticket provider to a computer of a prospective ticket consumer, data regarding an event for which tickets may be delivered; and then, the prospective ticket consumer deciding to obtain a ticket for a particular selected event and thus to become a ticket consumer,

first calculating in the computer of the ticket consumer a number **R**; then

25 second calculating in the computer of the ticket consumer a one-way function of the number **R** as **hash(R)**;

second transmitting, across the communications channel from the computer of the ticket consumer to the computer of the ticket provider, at least the **hash(R)** as ticket order data; and then, the ticket request being capable of being fulfilled,

10
15
20
25
30

third calculating in the computer of the ticket provider in respect of signature key **s** a digital signature of **hash(R)** appended to information **I** regarding the event as **Sign(s,I||hash(R))**, this **Sign(s,I||hash(R))** constituting a digital ticket precursor; then

5 third transmitting, across the communications channel from the computer of the ticket provider to the computer of the ticket consumer, the digital ticket precursor **Sign(s,I||hash(R))**;

fourth calculating, in the computer of the ticket consumer as an appending of **R** to the digital ticket precursor **Sign(s,I||hash(R))**, **Sign(s,I||hash(R))||R**, as a digital ticket;

10 first storing the digital ticket **Sign(s,I||hash(R))||R** from the computer of the ticket consumer to a transportable storage medium.

9. The method according to claim 8 expanded and extended to use of the digital ticket by the ticket consumer at the particular selected event, the method, after the writing, further comprising:

15 transporting the transportable storage medium within which the digital ticket **Sign(s,I||hash(R))||R** is written to the particular selected event;

20 tendering the digital ticket within the transportable storage medium for verification and for admission to the particular selected event;

reading the digital ticket **Sign(s,I||hash(R))||R** to an event computer;

25 extracting in the event computer the number **R** from the read **Sign(s,I||hash(R))||R**;

fifth calculating, by use of a verification key **v** complimentary to the signature key **s**, **I||hash(R)**; plus

sixth calculating in the event computer, with the same one-way function previously used in the second calculating, **hash(R)**; and then, having both **R** and sixth-calculated **hash(R)** to hand,

30 comparing the sixth-calculated **hash(R)** to the **hash(R)** portion

of the fifth-calculated $I || \text{hash}(R)$;

wherein IF the fifth-calculating proceeds correctly AND the information I is correct for the event AND the sixth-calculated $\text{hash}(R)$ compares to the fifth-calculated $\text{hash}(R)$ of the digital ticket as read THEN grant admission to a holder of the digital ticket ELSE IF the fifth-calculating proceeds incorrectly OR the information I is incorrect for the event OR the sixth-calculated $\text{hash}(R)$ fails to compares to the fifth-calculated $\text{hash}(R)$ of the digital ticket as read THEN deny admission to the holder of the digital ticket.

10. The method according to claim 9

wherein IF the fifth-calculating proceeds correctly AND the information I is correct for the event AND the sixth-calculated $\text{hash}(R)$ compares to the fifth-calculated $\text{hash}(R)$ of the digital ticket as read AND the read digital ticket is the first uniquely presented THEN grant admission to a holder of the digital ticket ELSE IF the fifth-calculating proceeds incorrectly OR the information I is incorrect for the event OR the sixth-calculated $\text{hash}(R)$ fails to compares to the fifth-calculated $\text{hash}(R)$ of the digital ticket as read OR the read digital ticket is not the first uniquely presented THEN deny admission to the holder of the digital ticket.

11. The method according to claim 9 that, between the extracting and the fifth calculating, further comprises:

second storing R in the event computer as an indication that the digital ticket has been tendered.

12. The method according to claim 8 where the ticket provider is also a ticket seller, the ticket consumer is also a ticket buyer, and the delivery of the ticket to the ticket consumer across the communications channel accompanies a sale of the ticket:

wherein the second transmitting further includes electronic payment suitable to the order data.

13. The method according to claim 8 wherein the first transmitting, the second transmitting and the third transmitting
5 are upon a worldwide communications network.

14. The method according to claim 8 wherein the first transmitting, the second transmitting and the third transmitting are upon a worldwide secure or encrypted communications network.

15. The method according to claim 14 wherein the first transmitting, the second transmitting and the third transmitting
10 are upon the Internet.

16. The method according to claim 15 wherein the first transmitting, the second transmitting and the third transmitting are upon the Secure Socket Layer (or SSL) of the Internet.

17. The method according to claim 8
15 wherein the first storing is in a transportable medium subsequently physically deliverable to the site of the particular selected event to there be tendered as a digital ticket by the ticket consumer.

20 18. The method according to claim 8 wherein the first storing is in the transportable medium of a printed substrate;

wherein the printed encrypted digital record is subsequently physically deliverable to the site of the particular selected event
25 to there be tendered as the digital ticket by the ticket consumer.

19. The method according to claim 18

wherein the first storing in the transportable medium of a printed substrate is in form of a two-dimensional bar code.

20. The method according to claim 19

5 wherein the first storing in the transportable medium of a printed two-dimensional bar code is in accordance with the PDF417 standard.

21. The method according to claim 19

10 wherein the first storing in the transportable medium of a printed two-dimensional bar code is in accordance with the QR standard.

22. The method according to claim 8

15 wherein the first storing in the transportable medium of a computer disk.

23. The method according to claim 8

20 wherein the first storing is in the transportable medium of a smart card;

wherein the digital record stored within the smart card is subsequently physically deliverable to the site of the particular selected event to there be tendered as the digital ticket by the ticket consumer.

~~24.~~ A system for delivering a digital ticket upon a communications network comprising:

25 a ticket consumer's computer, connected to the communications network,

for first transmitting ticket order data upon the communications network to a ticket provider's computer,

for first receiving upon the communications network from the ticket provider's computer a digitally signed ticket data, and

for storing the digitally signed ticket data in a transportable storage medium;

a ticket provider's computer, connected to the communications network,

5 for second receiving from the ticket consumer's computer upon the communications network the first-transmitted ticket order data,

for digitally signing the ticket data, and

10 for second transmitting the digitally signed ticket data upon the communications network to the ticket consumer's computer; and

a communications network

15 for communicating at a first time the first-transmitting of the ticket consumer's computer to the second-receiving of the ticket provider's computer, and

for communicating at a second time the fourth-transmitting of the ticket provider's computer to the first-receiving of the ticket consumer's computer.

20 25. The system for delivering a digital ticket according to claim 24

wherein the ticket consumer's computer

is first calculating a number **R**, and

is second calculating a one way function of **R** to produce **hash(R)** as ticket data,

25 wherein the first transmitting is of the second-calculated **hash(R)** as the ticket data,

wherein the first receiving is of **hash(R)** and additional information **I** digitally signed with signature key **s** as **Sign(s, I || hash(R))**,

30 is third calculating an appending of **R** to the digital ticket precursor **Sign(s, I || hash(R))**, giving **Sign(s, I || hash(R)) || R** as a digital ticket, and wherein the storing is of the

third-calculated digital ticket $\text{Sign}(s, I || \text{hash}(R)) || R$;

wherein the ticket provider's computer

is second receiving the first-transmitted $\text{hash}(R)$ ticket order data,

5 is calculating a digital signature in respect of the ticket data, and additional information I , in respect of signature key s as $\text{Sign}(s, I || \text{hash}(R))$, and

is second transmitting the calculated $\text{Sign}(s, I || \text{hash}(R))$.

26. The system for delivering a digital ticket according to claim 25

wherein the ticket consumer's computer is storing the digital ticket by printing it.

27. The system for delivering a digital ticket according to claim 26

wherein the ticket consumer's computer is storing the digital ticket by printing it in a 2-D machine-readable pattern.

28. The system for delivering a digital ticket according to claim 27

20 wherein the ticket consumer's computer is storing the digital ticket by printing it in a 2-D machine-readable bar code pattern.

29. A system for delivering a digital ticket upon a communications network comprising:

a ticket consumer's computer, connected to the communications network,

25 for first calculating a number R ,

for second calculating a one way function of R to produce $\text{hash}(R)$ as ticket data,

for first transmitting the second-calculated $\text{hash}(R)$ ticket data upon the communications network to a ticket provider's

computer as a ticket data for a particular selected event,

for first receiving upon the communications network a digitally signed data in respect of signature key **s** of **hash(R)** and additional information **I** as **Sign(s,I||hash(R))**,

5 for third calculating an appending of **R** to the digital ticket precursor **Sign(s,I||hash(R))** so as to give **Sign(s,I||hash(R))||R** as a digital ticket, and

for first storing the third-calculated digital ticket **Sign(s,I||hash(R))||R** in a transportable storage medium;

10 a ticket provider's computer, connected to the communications network,

for second receiving from the ticket consumer's computer upon the communications network the first-transmitted **hash(R)** ticket data,

for fourth calculating digitally signed data in respect of signature key **s** of second-received **hash(R)** and of information **I** as **Sign(s,I||hash(R))**, and

for second transmitting the fourth-calculated **Sign(s,I||hash(R))** upon the communications network to the ticket consumer's computer;

and a communications network

for communicating at a first time the first-transmitting of the ticket consumer's computer to the second-receiving of the ticket provider's computer, and

25 for communicating at a second time the fourth-transmitting of the ticket provider's computer to the first-receiving of the ticket consumer's computer.

30. A digital ticket comprising:

a tangible transportable data storage medium containing a digital signature of an issuer of the ticket.

31. The digital ticket according to claim 30 wherein the tangible

transportable data storage medium contains $\text{Sign}(s, I || \text{hash}(R)) || R$ where R is a random number private to the ticket consumer, $\text{hash}(R)$ is a one-way function of R , and $\text{Sign}(s, I || \text{hash}(R))$ is a digital signature, in respect of signature key s private to the ticket provider, of the $\text{hash}(R)$ appended to information I .

32. A digital ticket procured by a ticket consumer upon a communication network from and by interaction with a ticket provider, the digital ticket comprising:

a tangible transportable data storage medium containing $\text{Sign}(s, I || \text{hash}(R)) || R$ where R is a random number private to the ticket consumer, $\text{hash}(R)$ is a number that is a one-way function of R , and $\text{Sign}(s, I || \text{hash}(R))$ is a digital signature, in respect of signature key s private to the ticket provider, of the $\text{hash}(R)$ appended to information I .

33. A digital ticket procured by a ticket consumer upon a communication network from and by interaction with a ticket provider, the digital ticket comprising:

a tangible transportable data storage medium containing $\text{Sign}(s, I || \text{hash}(R)) || R$ where

(1) R is a number having its origin in a computer of the ticket consumer, which number R is appended to

(2) a number $\text{Sign}(s, I || \text{hash}(R))$ that was computed in a computer of the ticket provider as a digitally signature signed data in respect of a signature key s of a number $\text{hash}(R)$ appended to information I , thus $\text{Sign}(s, I || \text{hash}(R))$, and subsequently communicated across the communications network to the computer of the ticket consumer, which number $\text{hash}(R)$ was itself computed in the computer of the ticket provider consumer as a one way function of R , thus $\text{hash}(R)$, and subsequently communicated to the computer of the ticket provider;

wherein number R , having its origin in a computer of the

ticket consumer, is private to the ticket consumer and is not public; and

wherein the digital signature key *s* of the computer of the ticket provider is private to the ticket provider and is not public.

34. A digital ticket comprising:

a tangible transportable digital data storage medium containing

first-type data, originally known both to a buyer and to a seller of a ticket and meaningful to at least the seller of the ticket to identify, at least relatively, a particular event for which the ticket was sold, and

second-type data including a signed digital representation of a particular parameter that was originally computer-generated in sequence

first by the buyer of the ticket as a non-invertible function of a random number called a "first-time-made non-invertible function", and then

second by the seller of the ticket as a digital signature of the first-time-made non-invertible function, and then

third by the buyer of the ticket to attach the selfsame random number;

wherein, to validate the digital ticket upon attempted redemption of the ticket,

the random number is detached, and then

the signed first-time-made non-invertible function is interpreted, recovering this first-time-made non-invertible function, and then

the non-invertible function of that selfsame random number just detached is newly made all over again, which newly made non-invertible function is called the "second-time-made non-invertible function;

35. The digital ticket according to claim 34 wherein the digital signature within the tangible medium as read by a digital reader is further compared to a data base of digital tickets actually signed and sold not so as to determine whether a tendered digital ticket is valid or invalid but rather for statistical purposes.

36. The digital ticket according to claim 34 wherein the digital signature within the tangible medium is visible to the eye.

37. The digital ticket according to claim 34 wherein the digital signature visible to the eye is comparable by eye to a catalog of visual sensible representations of digital tickets actually signed and sold in order to determine whether a tendered digital ticket is valid or invalid.

38. A system for delivering a digital ticket from a ticket seller to a ticket buyer, the system comprising:

a communication channel for

at a first time sending from a ticket seller to a ticket buyer data regarding events for which tickets may be had,

at a second time sending from the ticket buyer to the ticket seller data representative of a non-invertible transformation of a number determined by the ticket buyer only, and

at a third time sending from the ticket seller to the ticket buyer a digital signature of the non-invertible transformation,

5

1987	1986	1985	1984	1983	1982
1981	1980	1979	1978	1977	1976
1975	1974	1973	1972	1971	1970
1969	1968	1967	1966	1965	1964
1963	1962	1961	1960	1959	1958
1957	1956	1955	1954	1953	1952
1951	1950	1949	1948	1947	1946
1945	1944	1943	1942	1941	1940
1939	1938	1937	1936	1935	1934
1933	1932	1931	1930	1929	1928
1927	1926	1925	1924	1923	1922
1921	1920	1919	1918	1917	1916
1915	1914	1913	1912	1911	1910
1909	1908	1907	1906	1905	1904
1903	1902	1901	1900	1899	1898
1897	1896	1895	1894	1893	1892
1891	1890	1889	1888	1887	1886
1885	1884	1883	1882	1881	1880
1879	1878	1877	1876	1875	1874
1873	1872	1871	1870	1869	1868
1867	1866	1865	1864	1863	1862
1861	1860	1859	1858	1857	1856
1855	1854	1853	1852	1851	1850
1849	1848	1847	1846	1845	1844
1843	1842	1841	1840	1839	1838
1837	1836	1835	1834	1833	1832
1831	1830	1829	1828	1827	1826
1825	1824	1823	1822	1821	1820
1819	1818	1817	1816	1815	1814
1813	1812	1811	1810	1809	1808
1807	1806	1805	1804	1803	1802
1801	1800	1799	1798	1797	1796
1795	1794	1793	1792	1791	1790
1789	1788	1787	1786	1785	1784
1783	1782	1781	1780	1779	1778
1777	1776	1775	1774	1773	1772
1771	1770	1769	1768	1767	1766
1765	1764	1763	1762	1761	1760
1759	1758	1757	1756	1755	1754
1753	1752	1751	1750	1749	1748
1747	1746	1745	1744	1743	1742
1741	1740	1739	1738	1737	1736
1735	1734	1733	1732	1731	1730
1729	1728	1727	1726	1725	1724
1723	1722	1721	1720	1719	1718
1717	1716	1715	1714	1713	1712
1711	1710	1709	1708	1707	1706
1705	1704	1703	1702	1701	1700
1699	1698	1697	1696	1695	1694
1693	1692	1691	1690	1689	1688
1687	1686	1685	1684	1683	1682
1681	1680	1679	1678	1677	1676
1675	1674	1673	1672	1671	1670
1669	1668	1667	1666	1665	1664
1663	1662	1661	1660	1659	1658
1657	1656	1655	1654	1653	1652
1651	1650	1649	1648	1647	1646
1645	1644	1643	1642	1641	1640
1639	1638	1637	1636	1635	1634
1633	1632	1631	1630	1629	1628
1627	1626	1625	1624	1623	1622
1621	1620	1619	1618	1617	1616
1615	1614	1613	1612	1611	1610
1609	1608	1607	1606	1605	1604
1603	1602	1601	1600	1599	1598
1597	1596	1595	1594	1593	1592
1591	1590	1589	1588	1587	1586
1585	1584	1583	1582	1581	1580
1579	1578	1577	1576	1575	1574
1573	1572				

5 a ticket buyer's computer, communicatively connected to the communications channel, for (i) determining the number, (ii) computing the non-invertible transformation, and (iii) combining the non-invertible transformation with the number to produce a digital ticket;

10 a ticket seller's computer, communicatively connected to the communications channel, for computing, in respect of the non-invertible transformation received from the buyer, the digital signature of the non-invertible transformation; and

15 a tangible portable medium of digital data storage connected to the buyer's computer for storing the digital ticket, and for transporting this digital ticket to a physical site of the particular selected event, where it may be used for admission.

39. The system according to claim 38 wherein the communication channel is sending at the second time a random number.

20 40. The system according to claim 38 wherein the communication channel is sending at the second time a number representing the particular selected event.

41. The system according to claim 38 wherein the communication channel comprises:

a worldwide digital communications network.

25 42. The system according to claim 38 wherein the communication channel comprises: a worldwide secure digital communications network.

43. The system according to claim 38 wherein the tangible portable

medium of digital data storage compris

[illegible]

a computer disk.

44. The system according to claim 38 wherein the tangible portable medium of digital data storage comprises:

5 a printed medium.

45. A printed ticket bearing indicia CHARACTERIZED IN THAT the indicia includes a 2-D bar code containing absolutely all necessary information by which the legitimacy, if not the uniqueness, of the ticket may be determined.

46. The printed ticket bearing indicia according to claim 45 FURTHER CHARACTERIZED IN THAT the 2-D bar coded indicia contains data digitally signed by the provider of the ticket.

47. The printed ticket bearing indicia according to claim 45 FURTHER CHARACTERIZED IN THAT the 2-D bar coded indicia contains a one-way function of a number provided by a holder of the ticket.

48. The printed ticket bearing indicia according to claim 45 FURTHER CHARACTERIZED IN THAT the 2-D bar coded indicia contains $\text{Sign}(s, I || \text{hash}(R)) || R$ where

(1) R is a number having its origin in a computer of a consumer of the ticket, which number R is appended to

(2) a number $\text{Sign}(s, I || \text{hash}(R))$ that was computed in a computer of a provider of the ticket as a digital signature in respect of digital signature key s of the number $\text{hash}(R)$ in combination with information I , subsequently communicated across the communications

computed in the computer of the ticket provider as a one

way function of R and subsequently communicated to the computer of the ticket provider;

wherein number R , having its origin in a computer of the ticket consumer, is private to the ticket consumer and is not public; and

wherein the digital signature key s of the computer of the ticket provider is private to the ticket provider and is not public.

49. A communications system for selling and delivering a digital ticket comprising:

a ticket buyer computer (i) sending at a first time a one-way transformation of a private number to a seller computer, (ii) receiving at a third time signed information from the ticket seller computer, and (iii) storing at a fourth time within a digital store the received encrypted signed information plus the private number;

a ticket seller computer (i) receiving at the first time the one-way transformation of the private number from the seller computer, (ii) signing at a second time this one-way transformation and additional information, and (iii) sending at the third time the signed first transformation and additional information to the ticket buyer computer as signed information; and

a digital store storing at the fourth time the signed information plus the private number as a digital ticket;

wherein upon (i) a reading of the signed information, (ii) a decrypting of the signed information to recover the one-way transformation of the private number, (iii) a reproducing with the same secure first transformation that the ticket seller used the secure first transformation of the number all over again, and (iv) a comparing of the decrypted recovered one-way transformation to the reproduced first transformation, validity of the digital ticket is assessable.

50. A method for selling and delivering a digital ticket comprising:

first-sending at a first time a one-way transformation of a private number from a ticket buyer computer to a ticket seller computer; first-receiving at the first time the one-way transformation of the private number in the ticket seller computer;

signing at a second time the one-way transformation and additional information in the ticket seller computer;

second-sending at a third time the signed first transformation and additional information as signed information from the ticket seller computer to the ticket buyer computer;

second-receiving at the third time the signed information in the ticket buyer computer;

storing with the ticket buyer computer at a fourth time both (i) the received signed information plus (ii) the private number within a digital memory store;

storing within the digital memory store at the fourth time the signed information plus the private number as a digital ticket;

wherein upon (i) a reading of the signed information, (ii) a decrypting of the signed information to recover the one-way transformation of the private number, (iii) a reproducing, with the same secure first transformation that the ticket seller used, the secure first transformation of the number all over again, and (iii) a comparing of the decrypted recovered one-way transformation to the reproduced first transformation, validity of the digital ticket is assessable.

51. In a communications system having a computer of a ticket buyer bi-directionally communicating across an insecure digital communications network to the secure computer of a ticket seller, a method for selling and for delivering a digital ticket from a ticket seller to a ticket buyer, the method comprising:

at a first time first-sending from the computer of the ticket

seller across the communications network to the computer of the ticket buyer first data regarding events for which tickets may be had; then at a second time

second-sending from the computer of the ticket buyer across the communications network to the computer of the ticket seller second data identifying an event for which a ticket is desired, the second data accompanied by a secure first transformation of a number that is determined by the ticket buyer only and unknown to others including the ticket seller; then at a third time

third-sending from the computer of the ticket seller across the communications network to the computer of the ticket buyer third data confirming ticketing to the event for which the ticket was desired, the third data accompanied by a secure second transformation of the secure first transformation; and then

storing, with the computer of the ticket buyer within a tangible portable medium of digital data storage, (i) the number in accompaniment to (ii) the secure second transformation;

wherein upon (i) transportation of the digital data storage medium to a physical site of the event, (ii) reading of the number to a computer, and, by use of the same secure first transformation that the buyer did use, reproduction of the secure first transformation of the number all over again, plus (iii) reversing of the secure second transformation by an event computer privileged to knowledge of said second transformation, then a (ii) read and reproduced first transformation is comparable to a (iii) first transformation recovered from reversing the second transformation in order to assess validity of the digital ticket.

52. The method according to claim 51 wherein the second-sending is of the second data accompanied by a secure first transformation in the form of a one-way hash function of the number.

53. The method according to claim 51 wherein the third-sending is

of the second data accompanied by a secure transformation in the form of a digital signature of the secure first transformation.

54. The method according to claim 51 wherein the storing within a tangible portable medium of digital data storage comprises:
5 printing.

55. The method according to claim 51 wherein the printing is of at least the (ii) secure second transformation in the form of a two-dimensional bar code.

56. The method according to claim 51 wherein the printing is of at least the (ii) secure second transformation in the form of a two-dimensional bar code.